

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-107084

(43)Date of publication of application : 21.04.1995

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

H04L 12/28

(21)Application number : 05-250852

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 06.10.1993

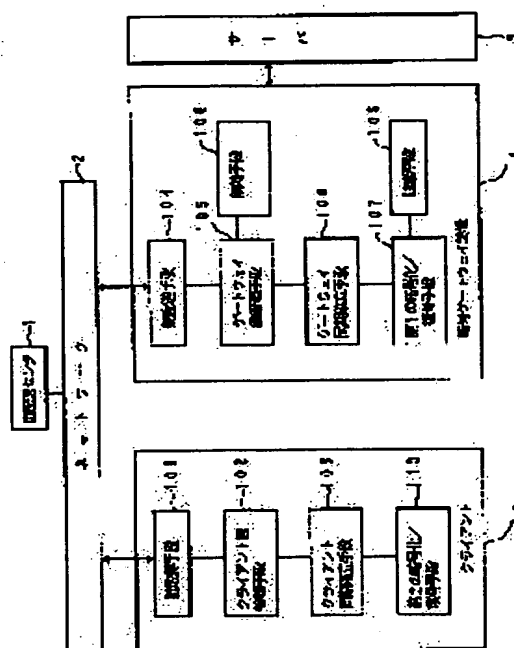
(72)Inventor : YAMAGUCHI TOSHIKAZU

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To provide a cipher communication system capable of performing cipher communication without influencing existing hardwares and application.

CONSTITUTION: A cipher gateway device 4 connected to a server 5 as a front-end processor establishes a session for communication between a client and the server with the detection of a cipher communication request from the client 3 as a trigger. At the time, with the detection of the cipher communication request from the client 3 as the trigger, the cipher gateway device 4 obtains a session key from a key delivery center 1, delivers it to the client 3 and shares the same session key between the client and the gateway device.



LEGAL STATUS

[Date of request for examination]

23.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3263879

[Date of registration]

28.12.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 特許公報 (B 2)

(11) 特許番号

特許第 3 2 6 3 8 7 9 号

(P 3 2 6 3 8 7 9)

(45) 発行日 平成14年3月11日 (2002. 3. 11)

(24) 登録日 平成13年12月28日 (2001. 12. 28)

(51) Int. Cl. ⁷ 識別記号
H 0 4 L 9/08
12/28

F I
H 0 4 L 9/00 6 0 1 B
11/00 3 1 0 Z

請求項の数 3

(全 1 4 頁)

(21) 出願番号 特願平5-250852
(22) 出願日 平成5年10月6日 (1993. 10. 6)
(65) 公開番号 特開平7-107084
(43) 公開日 平成7年4月21日 (1995. 4. 21)
審査請求日 平成10年10月23日 (1998. 10. 23)

(73) 特許権者 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72) 発明者 山口 利和
東京都千代田区内幸町1丁目1番6号 日本
電信電話株式会社内
(74) 代理人 100070150
弁理士 伊東 忠彦

審査官 青木 重徳

最終頁に続く

(54) 【発明の名称】 暗号通信システム

1

(57) 【特許請求の範囲】

【請求項 1】 ネットワークを介して複数のクライアントならびにサーバが鍵配送センタに接続され、該鍵配送センタが生成したセッション鍵を該ネットワークを介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、
該サーバと該ネットワークの間に位置し、サーバとの通信用セッションの確立時にクライアントが出力する暗号通信要求を検索し、該暗号通信要求を契機としてクライアントとの鍵配送用セッションを確立すると共に、該鍵配送センタからセッション鍵を取得し、該クライアントに配送する鍵配送手段と、取得した該セッション鍵を管理するゲートウェイ鍵管理手段と、該クライアントとの暗号同期を確立するゲートウェイ同期確立手段と、該同

2

期確立手段により同期完了報告後に該ゲートウェイ鍵管理手段より該セッション鍵を取得し、パケットを復号または暗号化する第1の暗号化／復号手段とを含む暗号ゲートウェイ装置と、
該サーバとの通信用セッション確立時に、該暗号ゲートウェイ装置に暗号通信を要求し、セッション鍵を取得する鍵取得手段と、取得した該セッション鍵を管理するクライアント鍵管理手段と、該暗号ゲートウェイ装置との暗号同期を確立するクライアント同期確立手段と、同期確立後、該クライアント鍵管理手段より該セッション鍵を取得し、パケットを復号または暗号化する第2の暗号化／復号手段とを含むクライアントを有し、
該クライアント・サーバ間の通信用セッション確立時に、該暗号ゲートウェイ装置が該クライアントからの暗号通信要求を検出してクライアントと鍵配送用セッション

ンを確立すると共に、該鍵配送センタから該セッション鍵を取得して、該クライアントに配送することにより、該クライアント・該暗号ゲートウェイ装置間で共通のセッション鍵を共有することを特徴とする暗号通信システム。

【請求項 2】 前記暗号ゲートウェイ装置は、前記クライアント・前記サーバ間の通信用セッション切断を検出し、前記ゲートウェイ鍵管理手段に保持する当該セッションのセッション鍵を無効にする無効手段を含む請求項 1 記載の暗号通信システム。

【請求項 3】 前記暗号ゲートウェイ装置は、前記クライアント・前記サーバ間で通信するパケットを受信し、前記クライアントと前記暗号ゲートウェイ装置間で暗号の同期確立が完了していないセッションのパケットを破棄する破棄手段を含む請求項 1 記載の暗号通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、任意のクライアントとサーバがセッションを確立し、共通鍵暗号アルゴリズムを用いて暗号通信を行う通信システムに係り、特に、ネットワークを介して複数のクライアント並びにサーバが鍵配送センタに接続され、鍵配送センタが生成したセッション鍵をネットワークを介して入手する暗号通信システムに関する。

【0002】

【従来の技術】図 1 2 は、従来の暗号通信システムの構成を示す。同図に示す従来の暗号通信システムは、ネットワーク 2 を介して、複数のクライアント 3₁ ~ 3₃ 及びサーバ 5 が鍵配送センタ 1 に接続され、鍵配送センタ 1 が生成したセッション鍵をクライアント 3 またはサーバ 5 が入手する。

【0003】図 1 3 は、従来の暗号通信システムを説明するための図である。同図 (A) は、鍵配送センタ 1 にセッション鍵を要求する場合に、クライアント 3 からアプリケーションプログラムを用いて要求する場合を示し、同図 (B) は、サーバ 5 からアプリケーションプログラムを用いて要求する場合を示す。このように、クライアント 3 またはサーバ 5 がアプリケーションプログラムを用いて通信に使用するセッション鍵を取得する。このセッション鍵をクライアント 3 とサーバ 5 間で共有し、以降の通信パケットをこのセッション鍵を用いて暗号化或いは、復号し、暗号通信を行う。

【0004】このように、従来の暗号通信システムは、広い地域に分散した事業所等の特定の端末間で暗号通信を行う LAN 等に効果的に利用できるものである。

【0005】

【発明が解決しようとする課題】しなしながら、上記従来の方式では、暗号通信に先立ち、クライアント或いはサーバ上で走行するアプリケーションプログラムが鍵配

送センタとセッションを確立し、鍵配送センタからセッション鍵を取得し、かつ通信相手のサーバ或いはクライアントのアプリケーションに同じセッション鍵を送信する処理が必要となる。

【0006】一方、コネクション型のネットワークを介して、クライアント・サーバ間で通信を行う通信プログラムの数は膨大であり、これらを暗号通信対応に変更する場合には、個別にアプリケーションプログラムやクライアント或いはサーバのハードウェアを改造する必要がある。改造規模や工数が大きくなり、これに伴って、開発費も大きくなるという問題がある。

【0007】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、既存のハードウェアやアプリケーションに影響を与えることなく、暗号通信を行うことができる暗号通信システムを提供することを目的とする。

【0008】

【課題を解決するための手段】図 1 は、本発明の原理構成図である。本発明は、ネットワーク 2 を介して複数のクライアント 3 ならびにサーバ 5 が鍵配送センタ 1 に接続され、鍵配送センタ 1 が生成したセッション鍵をネットワーク 2 を介して入手することにより、任意のクライアント 3・サーバ 5 間でセッションを確立して暗号通信を行う通信システムにおいて、サーバ 5 とネットワーク 2 の間に位置し、サーバ 5 との通信用セッションの確立時にクライアント 3 が出力する暗号通信要求を検索し、暗号通信要求を契機としてクライアント 3 との鍵配送用セッションを確立すると共に、鍵配送センタ 1 からセッション鍵を取得し、クライアント 3 に配送する鍵配送手段 104 と、取得したセッション鍵を管理するゲートウェイ鍵管理手段 105 と、クライアント 3 との暗号同期を確立するゲートウェイ同期確立手段 106 と、同期確立手段 106 により同期完了報告後にゲートウェイ鍵管理手段 105 よりセッション鍵を取得し、パケットを復号または暗号化する第 1 の暗号化／復号手段 107 とを含む暗号ゲートウェイ装置 4 と、サーバ 5 との通信用セッション確立時に、暗号ゲートウェイ装置 4 に暗号通信を要求し、セッション鍵を取得する鍵取得手段 101 と、取得したセッション鍵を管理するクライアント鍵管理手段 102 と、暗号ゲートウェイ装置との暗号同期を確立するクライアント同期確立手段 103 と、同期確立後、クライアント鍵管理手段 102 よりセッション鍵を取得し、パケットを復号または暗号化する第 2 の暗号化／復号手段 110 とを含むクライアント 3 を有し、クライアント・サーバ 5 間の通信用セッション確立時に、暗号ゲートウェイ装置がクライアント 3 からの暗号通信要求を検出してクライアント 3 と鍵配送用セッションを確立すると共に、鍵配送センタ 1 からセッション鍵を取得して、クライアント 3 に配送することにより、クライアント・暗号ゲートウェイ装置間で共通のセッション鍵を

共有する。

【0009】また、本発明の暗号ゲートウェイ装置4は、クライアント3・サーバ5間の通信用セッション切断を検出し、ゲートウェイ鍵管理手段105に保持する当該セッションのセッション鍵を無効にする無効手段108を含む。

【0010】また、本発明の暗号ゲートウェイ装置4は、クライアント3・サーバ5間で通信するパケットを受信し、クライアント3と暗号ゲートウェイ装置4間で暗号の同期確立が完了していないセッションのパケットを破棄する破棄手段109を含む。

【0011】

【作用】図2は、本発明の通信シーケンスの概要を示す。本発明は、サーバにフロントエンドプロセッサとして、暗号ゲートウェイ装置を接続し、この暗号ゲートウェイ装置がクライアントからの暗号通信要求の検出(ステップ1)を契機としてクライアント・サーバ間の通信用セッションを確立する(ステップ2)。このとき、暗号ゲートウェイ装置がクライアントからの暗号通信要求の検出を契機として、鍵配送センタからセッション鍵を取得(ステップ3)して、クライアントに配送する(ステップ4)ことにより、クライアント・ゲートウェイ装置間で同一のセッション鍵を共有する(ステップ5)。クライアントは暗号ゲートウェイ装置との暗号同期を確立し、これ以降、クライアント・サーバ間のセッションが切断されるまでクライアント・暗号ゲートウェイ装置間の暗号通信が可能となる(ステップ6)。

【0012】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【0013】図3は、本発明のシステム全体図である。同図に示す通信システムは、ネットワーク2を介して接続される鍵配送センタ1、クライアント3、暗号ゲートウェイ装置4、暗号ゲートウェイ装置4に接続されるサーバ5により構成される。同図において、サーバ5の前段に暗号ゲートウェイ装置4が接続されているが、クライアント3の前段に暗号ゲートウェイ装置4を接続することも考えられる。本実施例では、暗号ゲートウェイ装置4はサーバ5のフロントエンドとして接続されており、簡単のため、暗号ゲートウェイ装置4には1つのサーバ5が接続されるものとして説明する。

【0014】鍵配送センタ1は、セッション鍵を生成して暗号ゲートウェイ装置4に送信する。ネットワーク2は、クライアント3-サーバ5間、鍵配送センタ1-暗号ゲートウェイ装置4間、クライアント3-暗号ゲートウェイ装置4間でセッションを確立し、通信を行う。暗号化ゲートウェイ装置4は、クライアント3-サーバ間5でやり取りするパケットを暗号化/復号する。

【0015】図4は、本発明の一実施例のシステム構成図である。同図中、図3と同一構成部分には同一符号を

付す。同図に示すクライアント3は、セッション制御部31、セッション鍵配送部32、鍵管理部33、暗号同期確立部34、暗号化/復号部35、送信/受信部36から構成される。

【0016】セッション制御部31は、サーバ5との通信用セッション確立時に、プロトコルに暗号通信要求のメッセージを挿入し、暗号ゲートウェイ装置4に暗号通信要求を行う。セッション鍵配送部32は、暗号ゲートウェイ装置4と鍵配送用セッションを確立し、暗号ゲートウェイ装置4からセッション鍵を取得し、鍵管理部33に配送する。

【0017】鍵管理部33は、セッション鍵配送部32から受け取ったセッション鍵をセッション毎に管理する。暗号同期確立部34は、クライアント3と暗号ゲートウェイ装置4間でセッション鍵配送部32によるセッション確立を契機に暗号通信の同期を確立する。

【0018】暗号化/復号部35は、アプリケーションから受け取ったデータを、鍵管理部33が保持する当該セッション鍵を使用して暗号化、または、サーバ5から受け取った暗号化されたパケットを復号する。送信/受信部36は、ネットワーク2から(へ)暗号化されたパケットを受信(送信)する。

【0019】暗号ゲートウェイ装置4は、セッション確立/切断のモニタ部41、セッション鍵配送部42、鍵管理部43、暗号同期確立部44、暗号化/復号部47、送信/受信部45、及びセッション識別部46より構成される。

【0020】セッション確立/切断のモニタ部41は、クライアント3とサーバ5間で通信するパケットをモニタし、セッションの確立用パケットであり、かつヘッダのオプションに“暗号通信要求”のメッセージが挿入されているパケット及びセッション切断用パケットを検出する。また、クライアント3から暗号通信要求が出されていることをセッション鍵配送部42に通知する。さらに、セッション切断がある場合には、この旨を鍵管理部43に通知する。

【0021】セッション鍵配送部42は、セッション確立/切断のモニタ部41から報告される暗号通信要求を契機としてクライアント3との間で鍵配送用セッションを確立し、鍵配送センタ1からセッション鍵を取得し、クライアント3に配送する。また、セッション鍵を鍵管理部43に配送する。

【0022】鍵管理部43は、セッション鍵配送部42から受け取ったセッション鍵をセッション毎に管理するとともに、セッション確立/切断のモニタ部41から報告されるセッション切断を契機として当該セッション鍵を無効にする。

【0023】暗号同期確立部44は、クライアント3と暗号ゲートウェイ装置4間で暗号通信の同期を確立し、同期完了を暗号化/復号部47に報告する。

【0024】送信／受信部45は、クライアント3或いはサーバ5から（へ）パケットを受信（送信）する。

【0025】セッション識別部46は、送信／受信部45から受け取ったパケットのIPヘッダ及びTCPヘッダから送信元IPアドレス、送信元ポート番号、送信先IPアドレス及び送信先ポート番号を取り出し、セッション番号を識別する。

【0026】暗号化／復号化部47は、暗号同期確立部44から同期完了報告前に受信したパケットを破棄し、同期完了報告後のパケットについては、セッション識別部46から受け取ったセッション番号をキーとして鍵管理部43からセッション鍵を取得し、サーバ5宛のパケットであれば、当該パケットを復号し、クライアント3宛のパケットであれば、当該パケットを暗号化する。

【0027】図5は、TCP/IP・LANで使用するプロトコルをOSIの参照モデルに準拠して記述している。データリンクレイヤは、MAC (Media Access Control) プロトコル、ネットワークレイヤは、IP (Internet protocol)、トランスポートレイヤはTCP (Transmission Control Protocol) で実現されており、APは、TCPレイヤ間でセッションを確立する。

【0028】図6は、TCP/IP・LANに接続されたクライアント・サーバ間で通信する際に使用するパケット・フォーマットを示す。

【0029】パケットは、MACヘッダ (MAC_H)，IPヘッダ (IP_H) 及びTCPヘッダ (TCP_H) からなるヘッダと、APデータ及びパケット全体のフレームチェック・シーケンス (FCS) から構成される。暗号ゲートウェイ装置4がアプリケーションデータを暗号化／復号することにより、クライアント3と暗号ゲートウェイ装置4間で暗号通信を行う。アプリケーションデータを暗号化することにより、IPルータを介したネットワークを使用して通信を行うことができる。なお、送信側のIPアドレス (IPヘッダに規定) 及びポート番号 (TCPヘッダに規定) と受信側のIPアドレス及びポート番号によりクライアント・サーバ間のセッションが一意に決定される。暗号ゲートウェイ装置4のセッション識別部46はこのように、パケットの送信側のTCPヘッダ、IPヘッダと受信側のIPアドレス及びポート番号によりセッションを識別する。

【0030】図7は、TCPヘッダのフォーマットを示す。同図において“_”は本発明に直接関係しないので、説明は省略する。

【0031】“SRC_PORT”及び“DST_PORT”は各々発信元のポート番号、送信先のポート番号を示す。“CF_PORT”は、各々送信元のポート番号、送信先のポート番号を示す。“CF (制御フラグ)”は、“SYN: Synchronize flag (セッションの確立)”、“ACK: Acknowledgement flag (確認)”及び“FIN: Fin flag (セッションの切断)”等から構

成される。

【0032】セッションの確立には、“SYN”及び“ACK”が、切断には“FIN”及び“ACK”が使用される。

【0033】図8は、本発明の一実施例のセッション確立手順のシーケンスチャートである。クライアント3からのパケットにセッション確立のフラグ“SYN”がサーバ5に渡され (ステップ101)、サーバ5が“SYN”に対して、“ACK”により応答する。この場合、サーバ5は、“SYN+ACK”をクライアント3に渡す (ステップ102)。これに対して、クライアント3は、サーバ5に応答の“ACK”を通知する (ステップ103)。これにより、クライアント3とサーバ5間のセッションが確立する (ステップ104)。

【0034】図9は、本発明の一実施例のセッション切断手順のシーケンスチャートを示す。クライアント3からパケットにセッションの切断のフラグ“FIN”がサーバ5に渡されると (ステップ201)、サーバ5は、“ACK”により応答すると共に (ステップ202)、セッションの切断のための“FIN”をクライアント3に通知する (ステップ203)。クライアント3はサーバ5からの通知を受け取った旨をサーバに“ACK”により通知する (ステップ204)。これにより、クライアント・サーバ間のセッションが切断される (ステップ205)。

【0035】なお、セッションの確立／切断手順の詳細は、“上原「異機種接続とLAN絵とき読本、pp. 137～141、オーム社」”を参照されたい。

【0036】クライアント3から暗号ゲートウェイ装置4に対する暗号通信要求には、TCP或いは、IPヘッダのオプションを利用して、メッセージ (暗号通信要求) 送信する方法を利用できる。

【0037】図10は、本発明の一実施例の鍵配送手順を示すシーケンスチャートである。なお、クライアント3及び暗号ゲートウェイ装置4の暗号鍵 K_{c1} 及び K_{s1} は、各装置のインストール時に内部に保持しており、外部から見ることはできない。

【0038】同図中、 $K_s = d K_{c1} (C_{c1})$: K_s は暗号文 C_{c1} を暗号鍵 K_{c1} で復号した結果である。

【0039】 (手順1) クライアント3は、サーバ5と通信用セッションを確立する。この時、クライアント3のセッション制御部31は、パケットのTCPヘッダのオプションに“暗号通信要求”メッセージを挿入する (ステップ301)。

【0040】 (手順2) 暗号ゲートウェイ装置4のセッション確立／切断のモニタ部41は、クライアント・サーバ間で通信するパケットをモニタし (ステップ302)、セッション鍵配送部42において、セッション確立用でかつ“暗号通信要求”が挿入されたパケットを検出した場合に、クライアント3と鍵配送用セッションを

確立する(ステップ303)。

【0041】(手順3) クライアント3は、暗号ゲートウェイ装置4にクライアント3の識別子 ID_{c1} を送信する(ステップ304)。

【0042】(手順4) 暗号ゲートウェイ装置4は、鍵配送センタ1にアクセスし、鍵取得手順(ステップ305)(詳しくは、図11において説明する)によりクライアント3及び暗号ゲートウェイ装置4それぞれの暗号鍵(K_{c1} 及び K_{gw})で暗号化されたセッション鍵(C_{c1} 及び C_{gw})を鍵配送センタ1から受信する(ステップ

(ステップ306)。

【0043】(手順5) 暗号ゲートウェイ装置4の鍵管理部43は、鍵配送センタ1より受け取った C_{gw} を暗号ゲートウェイ装置4の暗号鍵 K_{gw} で復号し、セッション鍵 K_s を取得する(ステップ307)。セッション鍵 K_s は、サーバ5とのセッションを切断するまで保持される。

【0044】(手順6) 暗号ゲートウェイ装置4のセッション鍵配送部42は、クライアント3に鍵配送センタ1から受信したセッション鍵 C_{c1} を配送する(ステップ

308)。

【0045】(手順7) クライアント3は、暗号ゲートウェイ装置4からセッション鍵 C_{c1} (暗号)を受信する(ステップ309)。

【0046】(手順8) クライアント3は、自分の暗号鍵 K_{c1} を用いて暗号ゲートウェイ装置4から配送された C_{c1} を復号し、セッション鍵 K_s を取得する(ステップ

310)。

【0047】(手順9) クライアント3の暗号同期確立部34と暗号ゲートウェイ装置4の暗号同期確立部44は、暗号同期の確立を行う(ステップ311)。暗号同期の確立が完了すると、クライアント3は暗号ゲートウェイ装置4とのセッションを切断する(ステップ312)。なお、暗号同期の確立方法は、本発明の目的とするところではないので、詳細な説明は省略する。

【0048】(手順10)以降、共通のセッション鍵 K_s を用いて、クライアント3と暗号ゲートウェイ装置4間の暗号通信が可能となる(ステップ313)。

【0049】(手順11) 暗号ゲートウェイ装置4は、クライアント3からサーバ5宛のパケットを受信し、暗号化/復号部47でセッション識別部46により識別された該当するセッション鍵を使用して、パケットを復号する(ステップ314)。この復号されたパケット(平文のパケット)をサーバ5に送信することにより、暗号ゲートウェイ装置4とサーバ5間で非暗号通信が可能である(ステップ315)。

【0050】また、サーバ5からクライアント3宛のパケットについては、暗号ゲートウェイ装置4の暗号化/復号部47にて、パケットを暗号化する。即ち、サーバ5から暗号ゲートウェイ装置4に対して平文を送信し

(ステップ313')、暗号ゲートウェイ装置4の暗号化/復号部47にて暗号化し(ステップ314')、セッション鍵 K_s を用いて暗号ゲートウェイ装置4とクライアント3間の暗号通信を行う(ステップ315')。

【0051】図11は、本発明の一実施例の暗号ゲートウェイ装置の鍵配送センタからの鍵取得のシーケンスチャートである。

【0052】(手順1) 暗号ゲートウェイ装置4は、鍵配送センタ1とセッションを確立する(ステップ401)。

【0053】(手順2) 暗号ゲートウェイ装置4は、鍵配送センタ1にクライアント3及び暗号ゲートウェイ装置4の識別子 ID_{c1} 及び ID_{gw} を送信する(ステップ402)。なお、識別子 ID_{c1} 及び ID_{gw} は装置を識別するために使用するIPアドレス或いは、MACアドレスである。

【0054】(手順3) 鍵配送センタ1は、乱数を発生し、セッション鍵 K_s を生成する。さらに、クライアント及び暗号ゲートウェイ装置4の暗号鍵 K_{c1} 及び K_{gw} を識別子 ID_{c1} 、 ID_{gw} に基づいて検索(或いは生成)する。ここで、 K_{c1} 及び K_{gw} の検索(或いは生成)する方法は、本発明の直接的な目的ではないので説明を省略する。検索により K_{c1} 及び K_{gw} を取得する場合には、装置の識別子及び暗号鍵を鍵配送センタ1のデータベースに登録する手段が必要であることはいうまでもない。さらに、 K_{c1} 及び K_{gw} を生成する方法は、“小柳津、田中『UUIを利用した鍵配送方式、信学技報』、OFS92-31”を参照されたい。

【0055】上記に示す K_{c1} 及び K_{gw} を用いて、鍵配送センタ1は、 K_s を暗号化し、 C_{c1} 及び C_{gw} を生成する(ステップ403)。

【0056】(手順4) 鍵配送センタ1は、暗号ゲートウェイ装置4に C_{c1} 及び C_{gw} を送信する(ステップ404)。

【0057】(手順5) 暗号ゲートウェイ装置4は、鍵配送センタ1とのセッションを切断する(ステップ405)。

【0058】なお、本発明は、上記の実施例に限定されことなく、以下の点でも種々応用が可能である。

【0059】ここでは、暗号ゲートウェイ装置4と鍵配送センタ1間は、セッションを確立して通信を行う例を説明したが、UDPプロトコルを使用するコネクションレス型の通信を使用してもよいし、また、他の通信プロトコルを使用してもよいということは、いうまでもない。

【0060】さらに、本発明は、鍵配送アルゴリズムを特定したものではない。従って、送信するデータの内容(ここでは、 ID_{c1} 、 ID_{gw} 、 C_{c1} 及び C_{gw})を変更すれば、相手端末の認証ができることはいうまでもない。詳しくは、文献“小柳津、田中『UUIを利用した鍵配

送方式』、信学技報、OFS 9 2 - 3 1”を参照されたい。

【0061】上記実施例では、暗号ゲートウェイ装置 4 に 1 つのサーバが接続されているパターンを説明したが、1 つの暗号ゲートウェイ装置 4 に複数のサーバを接続することも考えられる。また、暗号ゲートウェイ装置 4 をサーバに接続したが、クライアント側に接続することも考えられる。

【0062】

【発明の効果】上述のように本発明によれば、暗号暗号ゲートウェイ装置がクライアントからの暗号通信要求を検出し、これを契機としてクライアントと鍵配送セッションを確立すると共に、鍵配送センタにアクセスし、通信に使用するセッション鍵を取得し、通信相手であるクライアントに当該セッション鍵を配送し、クライアントと暗号ゲートウェイ間で共通のセッション鍵を共有し、このセッション鍵を用いて暗号通信を行うため、従来のように、暗号通信対応に既存のアプリケーションやハードウェアを改造する必要がなく、経済化を図ることができる。

【図面の簡単な説明】

【図 1】本発明の原理構成図である。

【図 2】本発明の概要のシーケンスである。

【図 3】本発明のシステム全体図である。

【図 4】本発明の一実施例のシステム構成図である。

【図 5】TCP/IP・LANで使用するプロトコルを示す図である。

【図 6】TCP/IP・LANのパケット・フォーマットである。

【図 7】TCPのヘッダフォーマットである。

【図 8】本発明の一実施例のセッション確立手順のシーケンスチャートである。

【図 9】本発明の一実施例のセッション切断手順のシーケンスチャートである。

【図 10】本発明の一実施例の鍵配送手順を示すシーケンスチャートである。

【図 11】本発明の一実施例の暗号ゲートウェイ装置の鍵配送センタからの鍵取得のシーケンスチャートである。

【図 12】従来の暗号通信システムの構成を示す。

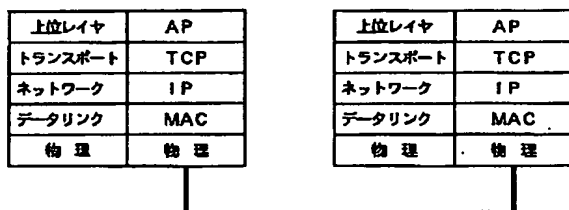
【図 13】従来の暗号通信システムを説明するための図である。

【符号の説明】

- 1 鍵配送センタ
- 2 ネットワーク
- 3 クライアント
- 4 暗号ゲートウェイ装置
- 5 サーバ
- 31 セッション制御部
- 32 セッション鍵配送部
- 33 鍵管理部
- 34 セッション鍵配送部
- 35 暗号化/復号部
- 36 送信/受信部
- 41 セッション確立/切断のモニタ部
- 42 セッション鍵配送部
- 43 鍵管理部
- 44 暗号同期確立部
- 45 送信/受信部
- 46 セッション識別部
- 47 暗号化/復号部
- 101 鍵取得手段
- 102 クライアント鍵管理手段
- 103 クライアント同期確立手段
- 104 鍵配送手段
- 105 ゲートウェイ鍵管理手段
- 106 ゲートウェイ同期確立手段
- 107 第 1 の暗号化/復号手段
- 108 無効手段
- 109 破棄手段
- 110 第 2 の暗号化/復号手段

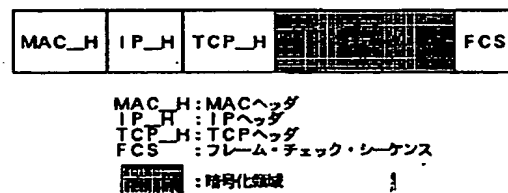
【図 5】

TCP/IP・LANで使用するプロトコルを示す図



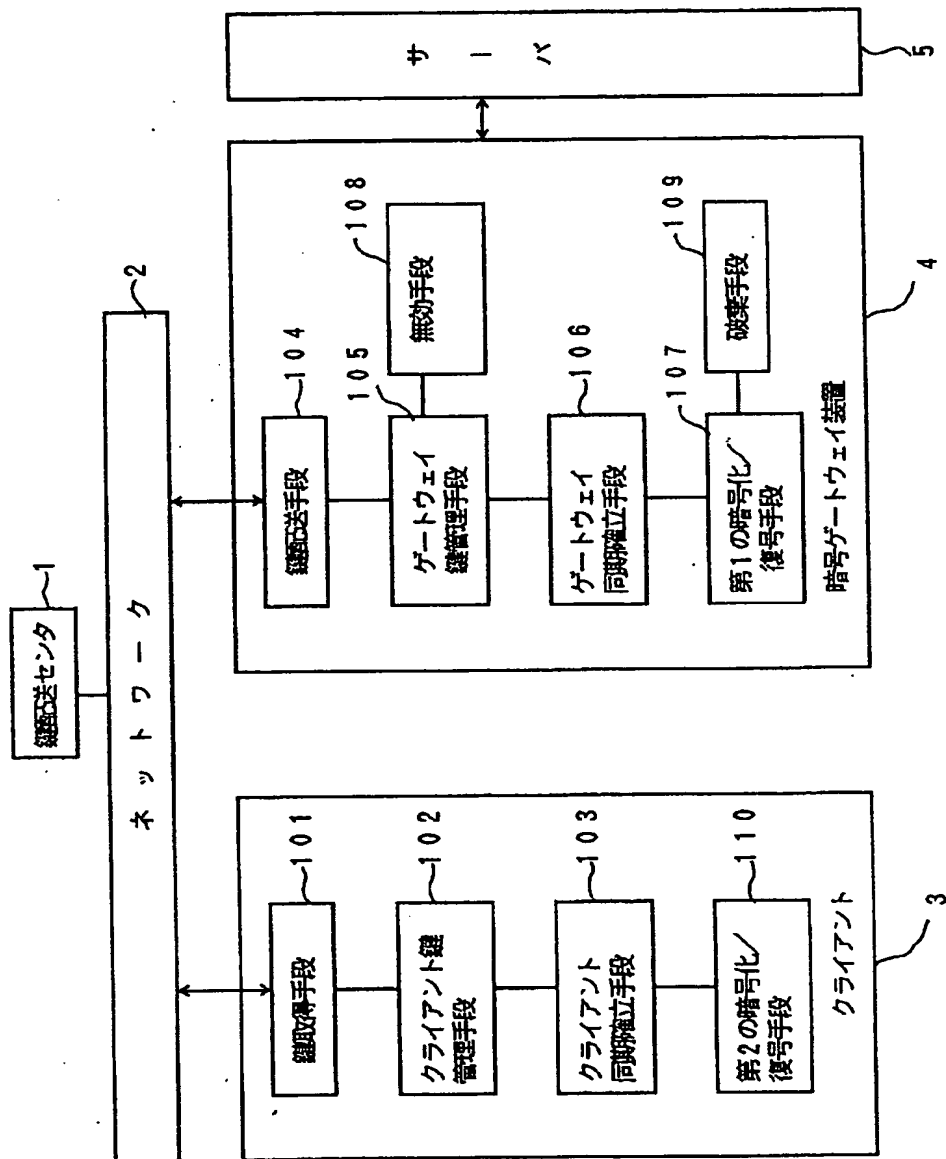
【図 6】

TCP/IP・LANのパケット・フォーマット



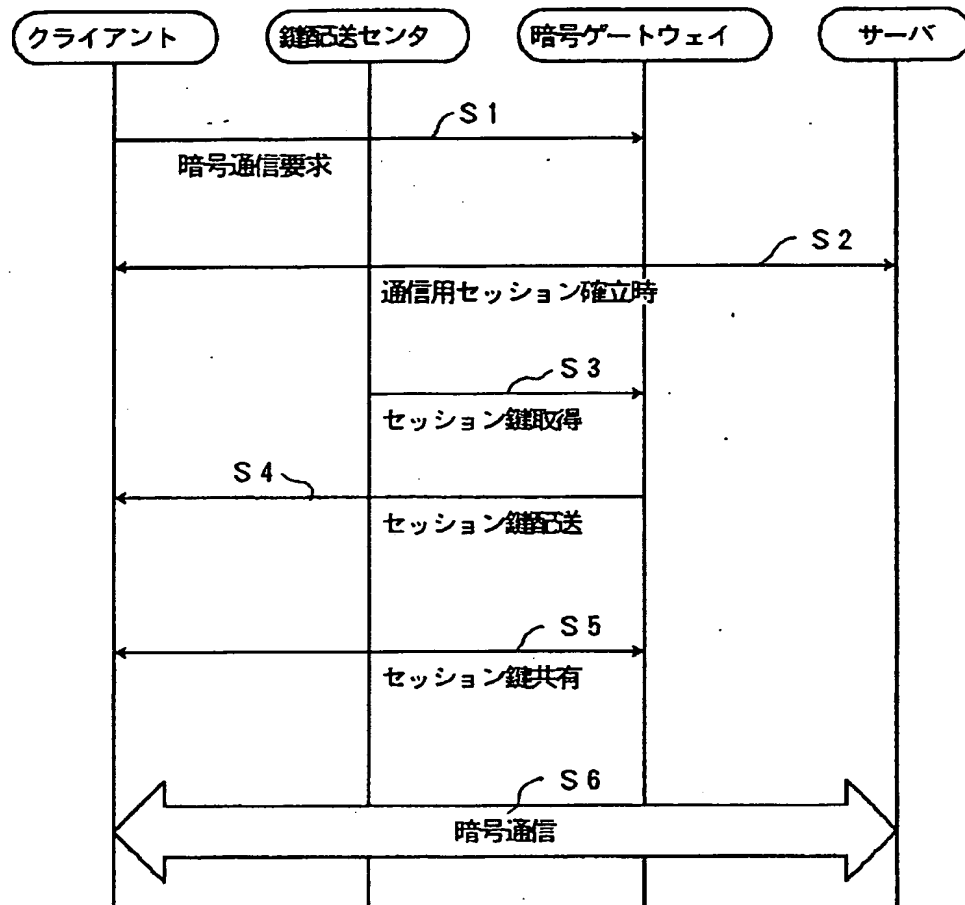
【図 1】

本発明の原理構成図



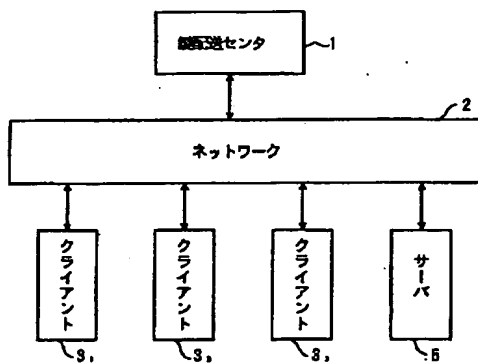
【図 2】

本発明の概要のシーケンス



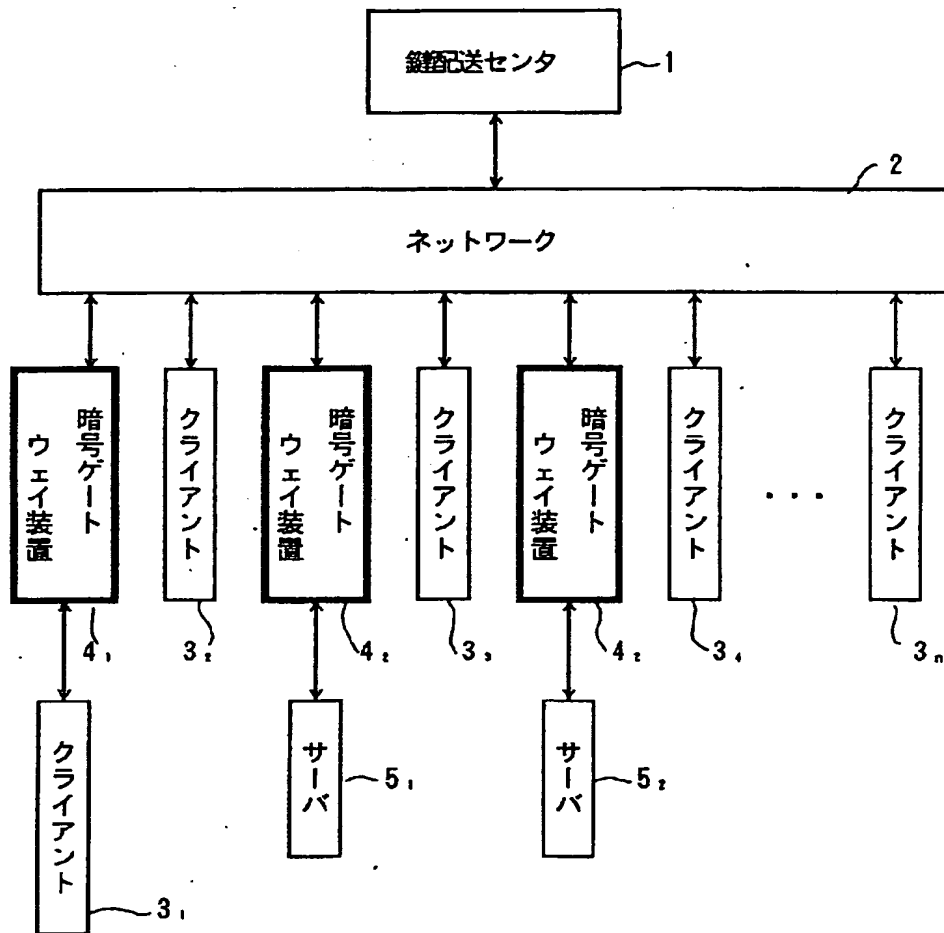
【図 1 2】

従来の暗号通信システムの構成図



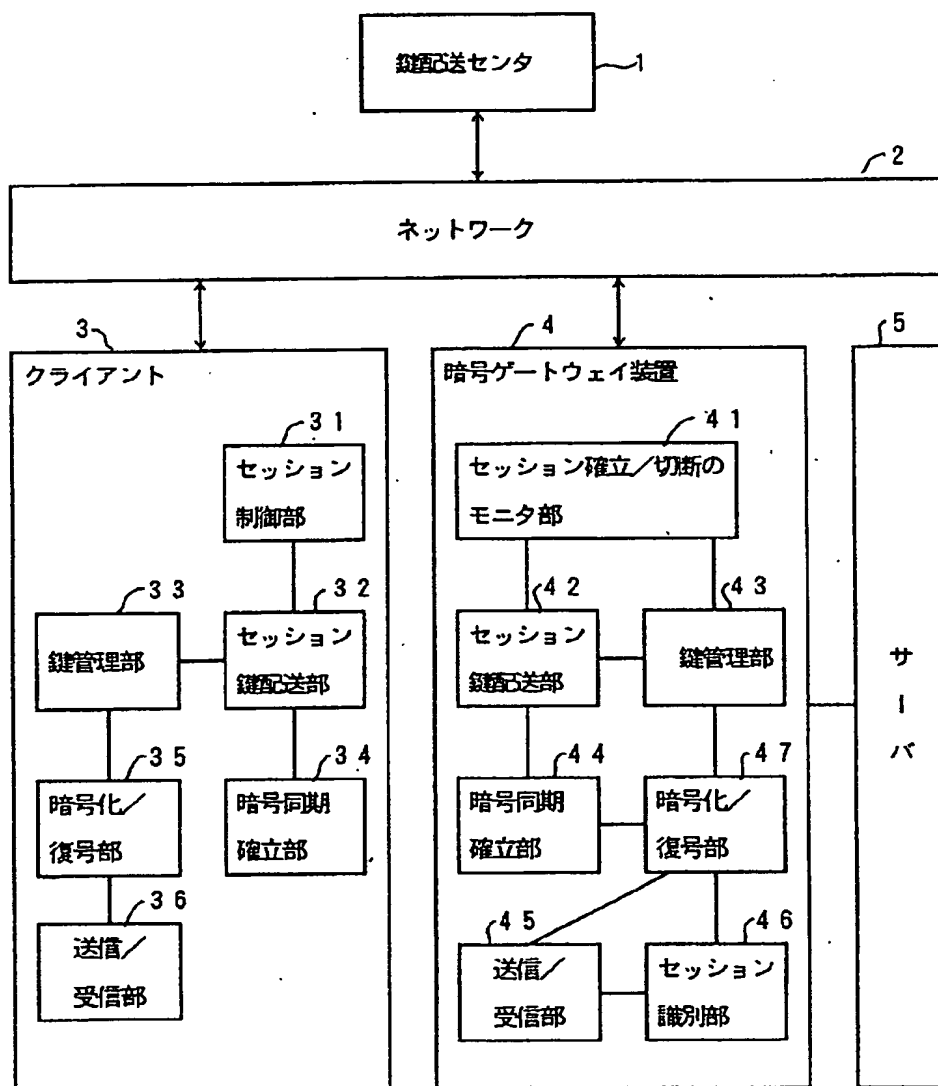
【図 3】

本発明のシステム全体図



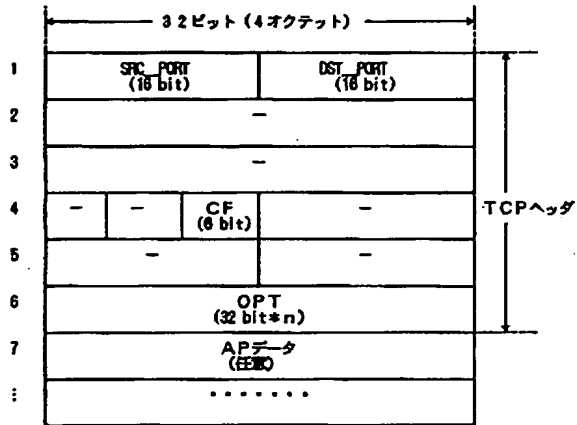
【図 4】

本発明の一実施例のシステム構成図



【図 7】

TCPヘッダのフォーマット



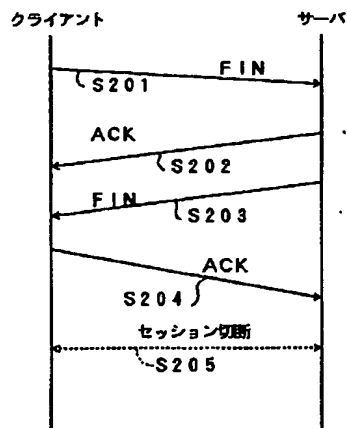
SRC_PORT : ソース・ポート
 DEST_PORT : デスティネーション・ポート
 CF : 制御フラグ



SYN (Synchronize Flag): セッションの確立
 ACK (Acknowledgment Flag): 確認
 FIN (Finish Flag): セッションの切断
 OPT : オプション

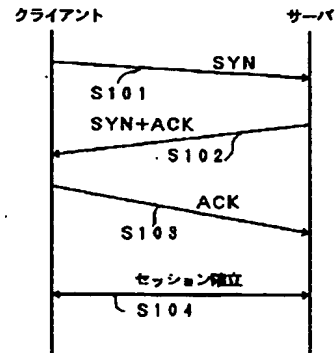
【図 9】

本発明の一実施例のセッション切断手段のシーケンスチャート



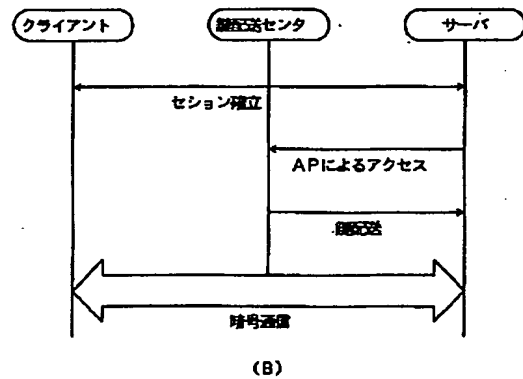
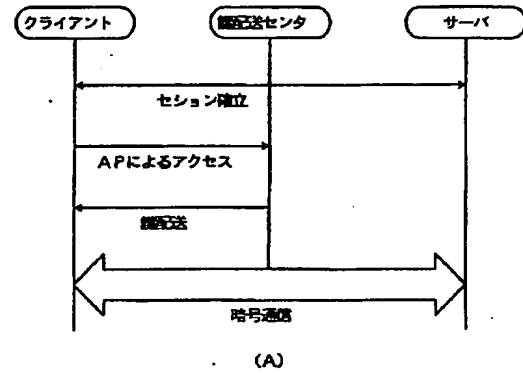
【図 8】

本発明の一実施例のセッション確立手段のシーケンスチャート



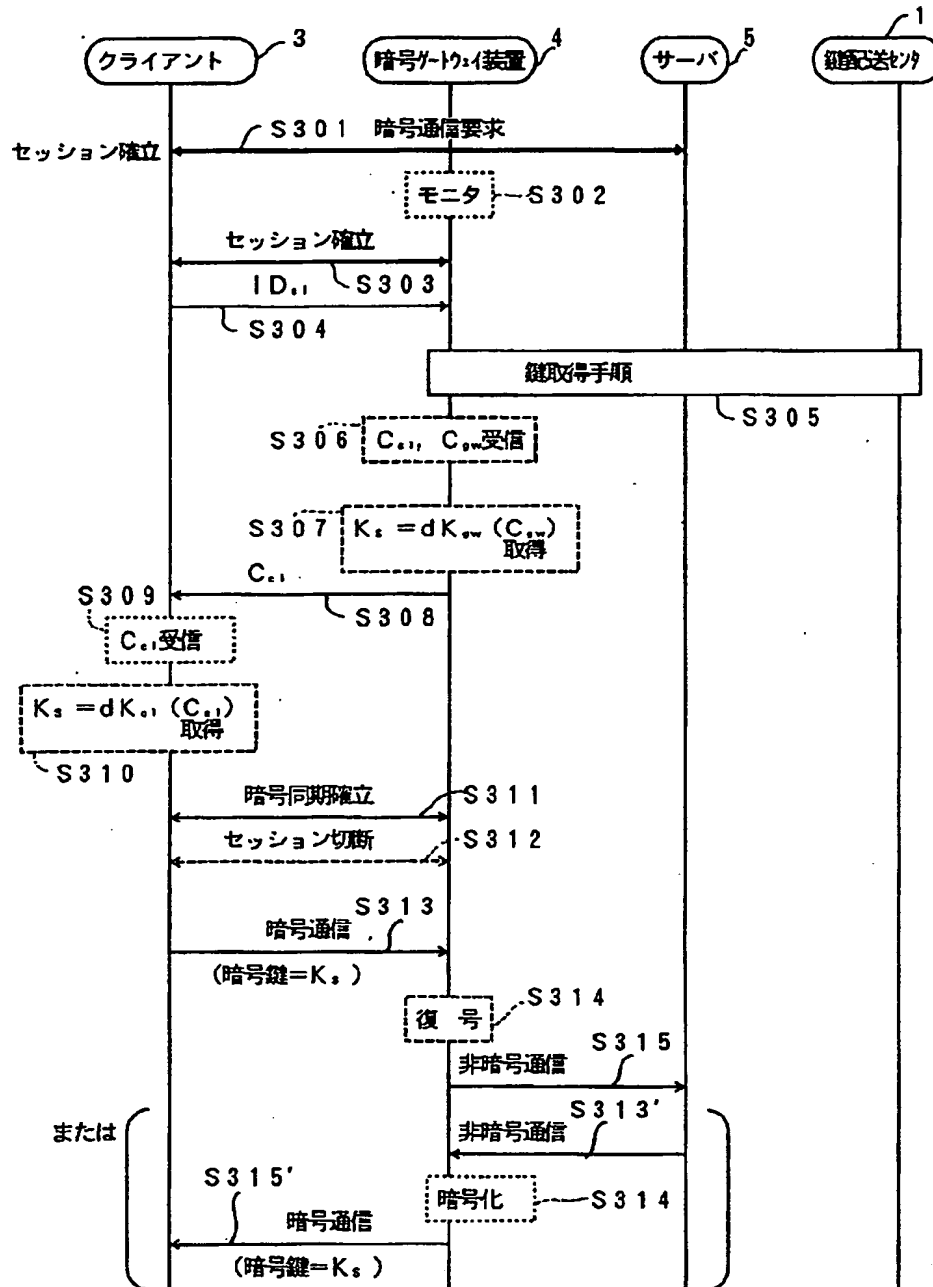
【図 13】

従来の暗号通信システムを説明するための図



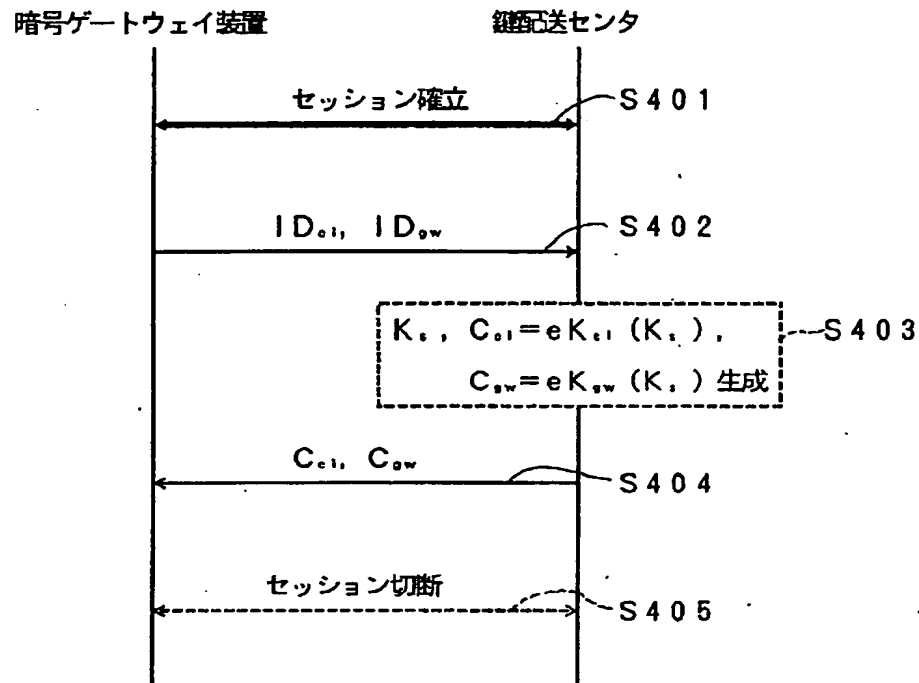
【図 10】

本発明の一実施例の鍵配送手段を示すシーケンスチャート

(注) $K_s = dK_{cl}(C_{cl})$: K_sは、暗号文C_{cl}を暗号鍵K_{sw}で復号した結果である。

【図 1 1】

本発明の一実施例の暗号ゲートウェイ装置の鍵配送
センタからの鍵取得のシーケンスチャート



(注) $C_{s,i} = eK_{s,i}(K_s)$: $C_{s,i}$ は平文 K_s を暗号鍵 $K_{s,i}$ で暗号化した結果である。

フロントページの続き

- (56) 参考文献 特開 昭63-274242 (J P, A)
特開 平4-179326 (J P, A)
特開 平7-107083 (J P, A)
山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LANの暗号通信における一方式, 電子情報通信学会技術研究報告 (O F S 93-32), 日本, 社団法人電子情報
通信学会, 1994年 1月21日, V o l .
93, N o . 435, p . 13-18
山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LAN暗号通信方式の実装と評価, 電子情報通信学会技術研究報告 (O F S 93-38), 日本, 社団法人電子情報
通信学会, 1994年 3月11日, V o l .
93, N o . 508, p . 7-12
山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LANセキュリティ通信技術-
TCPレイヤにおける通信データの暗号
化-, NTT R & D, 日本, 社団法人
電気通信協会, 1995年 7月 8日, V
o l . 44, N o . 9, p p . 653-660

- (58) 調査した分野(Int. Cl. 7, D B名)
H04L 9/08
H04L 12/28